

UNITED STATES BANKRUPTCY COURT DISTRICT OF NEW JERSEY Caption in Compliance with D.N.J. LBR 9004-1(b)	
BROWN RUDNICK LLP Robert J. Stark, Esq. Kenneth J. Aulet, Esq. Bennett S. Silverberg, Esq. Susan Sieger-Grimm, Esq. Seven Times Square New York, NY 10036 Telephone: (212) 209-4800 Fax: (212) 209-4801 Email: rstark@brownrudnick.com kaulet@brownrudnick.com bsilverberg@brownrudnick.com ssieger-grimm@brownrudnick.com <i>Proposed Counsel for the Official Committee of Unsecured Creditors</i> -and- GENOVA BURNS LLC. Daniel M. Stolz, Esq. Donald W. Clarke, Esq. Gregory S. Kinoian, Esq. 110 Allen Rd., Suite 304 Basking Ridge, NJ 07920 Telephone: (973) 230-2095 Fax: (973) 533-1112 Email: DStolz@genovaburns.com DClarke@genovaburns.com GKinoian@genovaburns.com <i>Proposed Local Counsel for the Official Committee of Unsecured Creditors</i>	BROWN RUDNICK LLP Stephen D. Palley, Esq. 601 Thirteenth Street, NW Washington, DC 20005 Telephone: (617)536-1766 Fax: (617)289-0466 Email: spalley@brownrudnick.com
In re: BLOCKFI INC., <i>et al.</i> , Debtors. ¹	Chapter 11 Case No. 22-19361 (MBK) Jointly Administered

¹ The Debtors in these Chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: BlockFi Inc. (0015); BlockFi Trading LLC. (2487); BlockFi Lending LLC (5017); BlockFi Wallet LLC (3231); BlockFi Ventures LLC (9937); BlockFi International Ltd. (N/A); BlockFi Investment Products LLC (2422); BlockFi Services, Inc. (5965) and BlockFi Lending II LLC (0154). The location of the Debtors' service address is 201 Montgomery Street, Suite 263, Jersey City, NJ 07302.

JOINDER OF THE OFFICIAL COMMITTEE OF UNSECURED CREDITORS TO DEBTORS' MOTION FOR ENTRY OF AN ORDER (I) AUTHORIZING THE DEBTORS TO FILE A CONSOLIDATED LIST OF TOP 50 UNSECURED CREDITORS AND CONSOLIDATED LIST OF CREDITORS, (II) AUTHORIZING THE DEBTORS TO REDACT CERTAIN PERSONALLY IDENTIFIABLE INFORMATION OF INDIVIDUAL CREDITORS, CLIENTS, EQUITY HOLDERS, AND CURRENT AND FORMER EMPLOYEES, (III) AUTHORIZING CLIENT NAME REDACTION, (IV) WAIVING THE REQUIREMENT TO FILE AN EQUITY LIST AND PROVIDE NOTICES DIRECTLY TO EQUITY SECURITY HOLDERS, AND (V) GRANTING RELATED RELIEF.

The Official Committee of Unsecured Creditors (the "**Committee**") appointed in the above-captioned Chapter 11 cases of BlockFi, Inc. and its affiliated debtors and debtors in possession (collectively, the "**Debtors**" or "**BlockFi**"), respectfully files this joinder to the *Debtors' Motion for Entry of an Order (I) Authorizing the Debtors to File a Consolidation List of Top 50 Unsecured Creditors and Consolidated List of Creditors, (II) Authorizing the Debtors to Redact Certain Personally Identifiable Information of Individual Creditors, Clients, Equity Holders, and Current and Former Employees, (III) Authorizing Client Name Redaction, (IV) Waiving the Requirement to File an Equity List and Provide Notices Directly to Equity Security Holders, and (V) Granting Related Relief* [Docket No. 4] (the "**Consolidation and Redaction Motion**"). The Committee also submits the Declaration of Maxwell Galka, attached hereto as **Exhibit A**, (the "**Galka Declaration**") in support of this joinder and states as follows:

PRELIMINARY STATEMENT

1. Sealing account holders' personally identifiable information is absolutely essential to protecting creditors of BlockFi, and the benefits of such protections should be beyond dispute. Hacking, identity theft, and harassment remain outsize risks in the cryptocurrency space, and disclosure of client names alone (let alone additional personally identifying information) significantly increases the risk of those clients being targeted for theft. These proceedings exist to

ameliorate, to the greatest extent possible, the harm caused to BlockFi's clients. There is no reason they should expose BlockFi's clients to further harm.

2. But the benefits of sealing likewise inure to the Debtors' Estates. The Debtors' going concern value remains opaque, but one thing remains perfectly clear: the Debtors' client list is one of their most valuable assets. If this information becomes publicly available, (a) actual and potential clients will lose even more trust in the Debtors, depleting any form of intrinsic value to such information, and (b) competitors will have access to the information, and potentially interested parties may find the Debtors a less attractive value proposition for a sale, new equity investment, or other restructuring transaction.

3. Law, equity, and financial common sense demand the protection of client identity information. The Consolidation and Redaction Motion should be granted.

Joinder

4. Cause exists to seal clients' personally identifying information pursuant to Section 107(c) of the Bankruptcy Code. Section 107(c) provides that the Court may protect an individual from disclosure of certain information if it finds that "disclosure of such information would create undue risk of identity theft or other unlawful injury to the individual[.]". The information encompassed by this provision includes "[a]ny means of identification (as defined in section 1028(d) of title 18) contained in a paper filed, or to be filed, in a case under this title" and "[o]ther information contained in a paper described in subparagraph (A)." "Means of identification" is defined as "any name or number that may be used, along or in conjunction with any other information, to identify a specific individual[.]" 18 U.S.C. 1028(d)(7).

5. BlockFi is in possession of a vast amount of confidential information belonging to account holders, including, but not limited to, their names, addresses, and e-mail addresses.

Undoubtedly, this information in the wrong hands can pose significant risks (both in terms of monetary loss and personal safety) to account holders. BlockFi account holders would be subject to an unreasonable risk of, among other things: (i) identity theft, (ii) verbal and physical harassment, (iii) theft and/or robbery, and (iv) hacking. *See* Galka Decl. ¶¶ 7-12.

6. These concerns are not merely hypothetical – there have unfortunately been severe consequences for account holders in the Celsius bankruptcy whose personal information was released. *See, e.g., Mack DeGeurin, New Tool Shows the Biggest Losers in the Celsius Crypto Meltdown*, Gizmodo, Oct. 10, 2022, available at <https://gizmodo.com/crypto-celsius-1849637951> (noting that searchable lists were created presumably from unredacted Celsius filings after the bankruptcy court made public approximately 14,000 pages of Celsius customer information, including their names and accompanying transaction histories).

7. Each aspect of a client’s personal identifying information poses serious risk due to the nature of digital assets. Once a transfer of a digital asset (e.g., bitcoin) is initiated, it cannot be reversed. *See* Galka Decl. ¶ 15. As a result, digital assets are a frequent target of hacking – a successful hack that initiates a transfer of the target’s digital assets is an effective form of online theft.

8. Because digital assets are such an attractive target for online theft, individuals known to possess digital assets face targeted hacking attempts. For example, one bitcoin core developer (presumably well-versed in online security) recently disclosed he had been the target of a concerted, personalized hacking campaign that resulted in the compromise of all of his bitcoin private keys and the theft of over 200 bitcoins – over \$3.6 million worth at the time of the hack.² BlockFi has significant numbers of retail clients who, presumably, have significantly less

² *See, e.g.,* <https://cointelegraph.com/news/bitcoin-core-developer-claims-to-have-lost-200-btc-in-hack>.

experience securing their systems against a determined attacker than a software developer who has worked on bitcoin for over a decade, and are thus at significantly greater risk if targeted for theft.

9. As a result, the mere disclosure of client names creates an unacceptable risk of theft to clients. *See* Galka Decl. ¶ 13. But that risk is massively increased if any additional personal information is released. *Id.* at ¶¶ 8-12. For example, each of the following pieces of information poses significant risks to clients, that would not be anticipated in an ordinary commercial bankruptcy case:

- a. **Email Addresses**: A person's email address is a 'skeleton key' to their entire online identity. Virtually any account can be accessed, without the password, if an attacker is in control of the target's email account: the attacker can initiate a password change (which, generally, requires only access to the password change email sent to the email address on file). Further, emails within that account will indicate where the client has accounts on other websites that might be worth attempting to hack. As a result, disclosure of a client's email address indicates to an attacker which email account they should target for compromise. Further, an email address can be used to search databases of password leaks to identify potential passwords to use in compromising accounts.
- b. **Phone Numbers**: Because passwords are commonly compromised, the "gold standard" for online security is two-factor authentication: requiring both a password **and** some additional authenticating detail. Most commonly, online companies rely on text messages (SMS) for the second factor: sending a one-time code to the cell phone number on file, to demonstrate control of that phone number as an additional layer of security. However, online attackers have begun to use so-called "SIM Swap" attacks to gain control of the target's phone number and intercept the SMS containing the code, thus bypassing the two-factor authentication.³ As a result, disclosure of client phone numbers discloses to an attacker which phone number they should target.
- c. **Mailing Address**: Because digital asset transfers are irreversible, a target can be physically compelled to transfer their digital assets. Further, if an individual keeps their digital assets in "cold storage" (i.e. not vulnerable to online theft) they can nonetheless be physically compelled to transfer them, or the computers containing those keys can be stolen. BlockFi operated

³ *See, e.g.,* An Empirical Study of Wireless Carrier Authentication for SIM Swaps, *available at* <https://www.usenix.org/system/files/soups2020-lee.pdf> (discussing how SIM swapping works, vulnerabilities in commonly-used systems, and noting that SIM swapping is commonly used to steal cryptocurrencies).

internationally, including in countries where such a risk is significantly higher than the United States.

10. Moreover, it is worth considering that information disclosure is never an isolated event. For instance, on December 22, 2022, data security firm LastPass announced a data breach that compromised client passwords for thousands of email addresses, online bank accounts, and other services. Widely used communications service Slack and software testing and delivery company CircleCI soon followed. *See Dan Goodin, “First LastPass, now Slack and CircleCI. The hacks go on (and will likely worsen)”*, Ars Technica, Jan. 5, 2023, available at <https://arstechnica.com/information-technology/2023/01/first-lastpass-now-slack-and-circleci-the-hacks-go-on-and-will-likely-worsen/>. Any BlockFi client who also uses these services (or whose data is compromised in any similar manner) would face significantly heightened risk of hacking and theft due to the potential for cross-referencing usernames and passwords with the addresses and financial records BlockFi seeks now to protect.

11. With account holders reeling from the instability of recent weeks (including many account holders losing access to all or a portion of their life savings), it is critical that the Court alleviate any further damage that may be done with release of account holders’ personally identifiable information.

12. Likewise, cause exists to seal client information under Section 107(b) of the Bankruptcy Code. Section 107(b) provides that “On request of a party in interest, *the bankruptcy court shall* ... protect an entity with respect to a trade secret or confidential research, development, or commercial information” (emphasis added). Commercial information is information that would result in “unfair advantage to competitors by providing them information as to the commercial operations of the debtor.” *In re Alterra healthcare Corp.*, 353 B.R. 66, 75 (Bankr. D. Del. 2006) (*citing In re Itel Corp.*, 17 B.R. 942, 944 (9th Cir. BAP 1982)).

13. If the Consolidation and Redaction Motion were not granted, not only would account holders be subject to the risks described herein, but any goodwill remaining with the Debtors would only be further eroded. This would diminish the value of the BlockFi brand to any potential purchaser and dilute (if not destroy) the value of the list and the client relationships inherent thereto. As such, disclosure would result in a potentially significant loss of enterprise value to the detriment of all stakeholders. *See Liveware Publishing, Inc., v. Best Software, Inc.*, 252 F.Supp.2d 74, 85 (D. Del. 2003) (customer list “is precisely the type of business information which is regularly accorded trade secret status”).

14. Notwithstanding cause for relief, the proposed order accompanying the Consolidation and Redaction Motion nonetheless provides various parties full access to the relevant account holder information. In addition to the Court, the U.S. Trustee, the SEC, and this Committee, the Debtors have offered to provide the information to any party in interest upon a request that is reasonably related to these Chapter 11 cases. This adequately balances the need for the public’s right to disclosure in these Chapter 11 cases against the need to ensure the safety of the Debtors’ account holders.

15. For the foregoing reasons, the Court should grant the Consolidation and Redaction Motion.

[Remainder of page intentionally left blank.]

WHEREFORE, this Court should grant the Consolidation and Redaction Motion, overrule any objection thereto, and grant related relief.

Respectfully submitted,

GENOVA BURNS LLC

By: /s/Donald W. Clarke

Daniel M. Stolz, Esq.

Donald W. Clarke, Esq.

Gregory S. Kinoian, Esq.

110 Allen Road, Suite 304

Basking Ridge, NJ 07920

Tel: 973-467-2700

Fax: 973-467-8126

Email: dstolz@genovaburns.com

dclarke@genovaburns.com

gkinoian@genovaburns.com

*Proposed Local Counsel to the Official
Committee of Unsecured Creditors*